PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-274999
(43)Date of publication of application : 08.10.1999

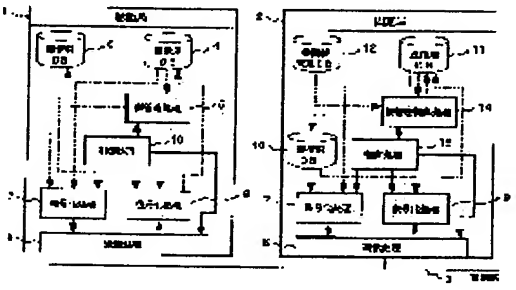
(51)Int.Cl. H04B 7/26
G07B 15/00
G07B 15/00
H04L 9/08

(21)Application number : 10-076909
(22)Date of filing : 25.03.1998

(71)Applicant : HITACHI LTD
HITACHI INF & CONTROL SYST LTD
(72)Inventor : NOZATO MASAYA
KAYUKAWA SATORU
IINO TAKAYUKI
ORIMO MASAYUKI
FUKUZAWA YASUKO
ISHIDA SHUICHI

(54) MOBILE COMMUNICATION METHOD AND MOBILE COMMUNICATION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a mobile communication system where the start of communication between a mobile station and a stationary station is quickened and a key in use is quickly and securely switched against an illegal use of an encryption key or the like.
SOLUTION: Common keys with plural versions are available for encryption communication between a stationary station and plural mobile stations, each mobile station 1 manages a sole key version and its symmetrical key (ordinary key and emergency key) in a form of key information DB 6, and the stationary station 2 manages plural key versions and their symmetrical keys in a way of key information management DB 12. The mobile station 1 sends a key version of its own station on a communication request, the stationary station 2 discriminates whether or nor a usual key of the received key version is effectively supported and replies the version and the key application (normal), when it is effectively supported. When the usual key is invalid, the stationary station 2 replies the version and the key application (urgent). The mobile station 1 discriminates the key version and the key application replied from the stationary station 2 and switches the key used by its own station into the urgent key, even if the key version is the same when the key application is the 'urgent key'.



LEGAL STATUS
[Date of request for examination] 09.08.2000
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number] 3445490
[Date of registration] 27.06.2003
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of

rejection]
[Date of extinction of right]

[0017]

Further, the stationary station, when the received version from the mobile station is included in the versions managed by its own station and the usual key is invalid, decides an alternative key paired with the usual key as a use key, replies the version and the key application (for alternative) to the mobile station that sends the communication request, as well as relates and manages an identifier of the mobile station and the use key during communication, and the mobile station, when the key application replied from the stationary station is for alternative, invalidates usual key of its own station and decides an alternative key paired with the usual key as a use key for cipher communication of its own station.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開平11－274999
(43)公開日　平成11年(1999)10月８日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｂ　7/26		Ｈ０４Ｂ　7/26	Ｒ
Ｇ０７Ｂ　15/00		Ｇ０７Ｂ　15/00	Ｊ
			Ｈ
	５１０		５１０
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ｅ

審査請求　未請求　請求項の数10　ＯＬ　（全 11 頁）　最終頁に続く

(21)出願番号　特願平10－76909
(22)出願日　平成10年(1998)３月25日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(71)出願人　000153443
株式会社日立情報制御システム
茨城県日立市大みか町５丁目２番１号
(72)発明者　野里　雅哉
茨城県日立市大みか町五丁目２番１号　株式会社日立情報制御システム内
(72)発明者　粥川　悟
茨城県日立市大みか町五丁目２番１号　株式会社日立情報制御システム内
(74)代理人　弁理士　高橋　明夫　（外１名）

最終頁に続く

(54)【発明の名称】　移動体通信方法および移動体通信システム

(57)【要約】
【課題】移動局と固定局間の通信開始を高速化し、また暗号鍵の不正使用等に対し速やかに且つ安全に使用鍵を切り替える移動体通信方式を提供する。
【解決手段】固定局と複数の移動局間の暗号通信に、複数のバージョンによる共通鍵を使用可能とし、各々の移動局１は唯一の鍵バージョンとその対称鍵（通常鍵と緊急鍵）を鍵情報ＤＢ６に管理し、固定局２は複数の鍵バージョンとその対称鍵を鍵情報管理ＤＢ１２に管理する。移動局１は通信要求時に自局の鍵バージョンを送信し、固定局２は受信した鍵バージョンの通常鍵が有効にサポートされているか判定し、有効な場合は当該バージョンと鍵用途（通常）を応答する。また、通常鍵が無効な場合は、当該バージョンと鍵用途（緊急）を応答する。移動局１は固定局２から応答された鍵バージョンと鍵用途を判定し、鍵バージョンが同じでも鍵用途が「緊急」の場合は、自局の使用鍵を緊急鍵に切り替える。

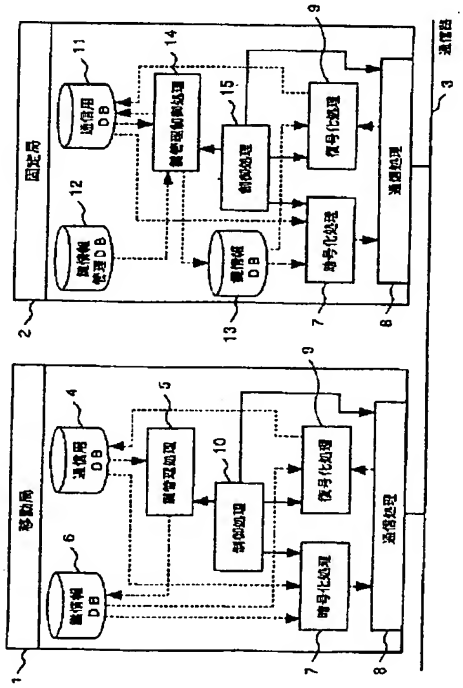


図１

【特許請求の範囲】

【請求項１】　固定局と移動局との双方向の暗号通信の暗号化または復号化に用いる鍵（暗号鍵）を複数の移動局で共有可能とし、かつ前記鍵の複数のバージョンを共用可能とする移動体通信方法において、

移動局は固定局への通信要求時に、自局の使用可能な暗号鍵のバージョンを送信すると共に、このバージョンが固定局からの応答に含まれることを確認し、

固定局は移動局からの受信バージョンが自局の管理する鍵情報に含まれるかチエックし、含まれる場合は当該バージョンを使用鍵に決定して前記通信要求を発信した移動局に応答すると共に、通信中、当該移動局の識別子とその使用鍵を対応付けて管理することを特徴とする移動体通信方法。

【請求項２】　請求項１において、

固定局は、移動局からの受信バージョンが自局の管理する鍵情報に含まれていない場合は、有効な鍵情報の一つまたはダミーのバージョンを移動局に応答し、当該移動局は、固定局からの応答バージョンが自局で使用可能な場合はそれによる通信要求を再送信することを特徴とする移動体通信方法。

【請求項３】　固定局と移動局との双方向の暗号通信の暗号化または復号化に用いる暗号鍵を複数の移動局で共有可能とし、かつ前記暗号鍵の複数のバージョンを共用可能とする移動体通信方法において、

各移動局及び固定局はそれぞれ自局の使用可能なバージョンの暗号鍵を、通常用と代替用の鍵用途に対応した一対の鍵（通常鍵と代替鍵）により管理し、

移動局は固定局への通信要求時に、自局の使用可能な暗号鍵のバージョンを送信すると共に、固定局からの応答に含まれるバージョンと鍵用途をチエックし、応答のバージョンが自局と同一で鍵用途が通常用の場合は、自局の通信に使用する暗号鍵を前記通常鍵のままとし、

固定局は移動局からの受信バージョンが自局の管理する複数のバージョンに含まれるかチエックし、含まれる場合は前記通常鍵の有効／無効をチエックし、有効の場合は当該通常鍵を使用鍵に決定して当該バージョンと鍵用途（通常用）を前記通信要求を発信した移動局に応答すると共に、通信中、当該移動局の識別子とその使用鍵を対応付けて管理することを特徴とする移動体通信方法。

【請求項４】　請求項３において、

固定局は、移動局からの受信バージョンが自局の管理するバージョンに含まれかつ前記通常鍵が無効の場合に、当該通常鍵と対をなす代替鍵を使用鍵に決定して当該バージョンと鍵用途（代替用）を前記通信要求を発信した移動局に応答すると共に、通信中、当該移動局の識別子とその使用鍵を対応付けて管理し、

当該移動局は、固定局から応答の鍵用途が代替用の場合に、自局の通常鍵を無効とし、それと対をなす代替鍵を自局の暗号通信の使用鍵とすることを特徴とする移動体通信方法。

【請求項５】　固定局と移動局との双方向の暗号通信の暗号化または復号化に用いる暗号鍵を複数の移動局で共有可能とし、かつ前記暗号鍵の複数のバージョンを共用可能とする移動体通信方法において、

各移動局及び固定局はそれぞれ自局の使用可能なバージョンの暗号鍵を、通常用と代替用の鍵用途に対応した一対の鍵（通常鍵と代替鍵）により管理し、

移動局は固定局への通信要求時に、自局の使用可能な暗号鍵のバージョンと鍵用途（通常または代替）を送信すると共に、固定局からの応答に含まれるバージョンをチエックし、応答のバージョンが自局と同一の場合は、自局から送信した鍵用途の暗号鍵を使用し、

固定局は移動局から受信したバージョンが自局の管理する複数のバージョンに含まれる場合に、受信した鍵用途が通常であれば前記通常鍵の有効／無効をチエックし、有効の場合は通常鍵を、無効の場合は前記代替鍵を使用鍵に決定し、受信したバージョンを前記通信要求を発信した移動局に応答すると共に、通信中、当該移動局の識別子とその使用鍵を対応付けて管理することを特徴とする移動体通信方法。

【請求項６】　請求項３、４または５において、

固定局における前記通常鍵の有効／無効の管理は、上位装置から指定されたバージョンの鍵用途変更指示を受信したときに、当該通常鍵を無効とすることを特徴とする移動体通信方法。

【請求項７】　通信処理手段と暗号化・復号化処理手段を有する固定局と、移動体上に搭載され通信処理手段と暗号化・復号化処理手段を有する複数の移動局を備え、移動局と固定局の双方向の暗号通信に用いる暗号鍵を複数の移動局で共有可能とし、かつ前記暗号鍵の複数のバージョンを共用可能とする移動体通信システムにおいて、

移動局は、自局の通信に使用する鍵バージョンと鍵を含む鍵情報を格納する鍵情報データベースと、固定局への通信要求時に自局の鍵バージョンを送信すると共に、固定局からの応答に含まれる鍵バージョンと対照して自局の使用鍵を管理する鍵管理処理手段を設け、

固定局は、移動局との通信に使用する複数の鍵バージョンとその鍵を含む鍵情報を格納する鍵情報管理データベースと、移動局から受信した鍵バージョンが前記鍵情報管理データベースに含まれる場合に当該鍵バージョンの鍵を使用鍵に決定して、当該鍵バージョンを移動局に応答する鍵管理制御処理手段と、通信中の移動局の識別子とその使用鍵を対応付けて管理する通信鍵情報データベースを設けることを特徴とする移動体通信システム。

【請求項８】　請求項７において、

固定局及び移動局は、前記鍵情報として鍵バージョン毎に通常／代替の鍵用途と対応する一対の通常鍵と代替鍵を含み、かつ固定局には、上位からの鍵用途変更指示に

よって該当鍵バージョンの通常鍵の使用を無効にする管理機能を有し、
固定局の前記鍵管理制御処理手段は、移動局から受信した鍵バージョンの通常鍵が無効の場合に対の代替鍵を使用鍵に決定してその鍵バージョンと鍵用途（代替）を移動局に応答し、移動局の前記鍵管理処理手段は固定局から応答の鍵用途が代替用の場合に鍵情報データベースの通常鍵を無効にすることを特徴とする移動体通信システム。
【請求項９】　請求項７において、
移動局は前記鍵情報として鍵バージョン毎に通常／代替の鍵用途と対応する一対の通常鍵と代替鍵を含み、
固定局は前記鍵情報として鍵バージョン毎に通常の鍵用途となる通常鍵を含み、かつ上位から鍵用途変更指示による鍵バージョンと鍵用途が代替の代替鍵を受信して管理すると共に当該通常鍵の使用を無効にする管理機能を有し、
固定局の前記鍵管理制御処理手段は、移動局から受信した鍵バージョンの通常鍵が無効の場合に前記代替鍵を使用鍵に決定してその鍵バージョンと鍵用途（代替）を移動局に応答し、移動局の前記鍵管理処理手段は固定局から応答の鍵用途が代替用の場合に鍵情報データベースの通常鍵を無効にすることを特徴とする移動体通信システム。
【請求項１０】　請求項７、８または９において、
前記移動体通信システムは有料道路の自動料金収受システムであり、前記固定局は料金所または路側に設けられる通信装置、前記移動局は有料道路を利用する車両に搭載される通信装置により構成される移動体通信システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は暗号通信方法に関し、特に固定局と移動局間で秘密にかつ耐改竄に暗号鍵を管理する移動通信に関する。
【０００２】
【従来の技術】携帯電話や自動車電話による移動通信の普及がめざましく、有料道路の自動料金収受システム（ＥＴＣ）などの実用化も間近かである。有料道路の自動料金収受システムは、料金所路側に設置された固定通信手段（固定局）と有料道路を走行する車両に搭載された移動通信手段（移動局）の間で、無線通信を用いて料金を収受するシステムである。ＥＴＣの課金処理では、利用者の認証や預金情報など個人のプライバシーに関する情報を無線で送受信するので、これら情報の漏洩、改竄を防止するために暗号通信を用いたセキュリティの確保が必須となる。
【０００３】通信内容の秘密保持や改竄の防止のために、平文を暗号化し暗号文を復号化するための鍵情報が使用される。例えば、『「インターネットセキュリティ」基礎と対策技術（佐々木良一他著，オーム社，ｐｐ９５－１０２）』に記載のように、送信者と受信者間で予め、ＫＥＫ(Key Encrypting Key)と呼ばれる「鍵暗号化鍵」を設定し、送信者はこのＫＥＫを用いてデータを暗号化するＤＥＫ(Data Encrypting Key)と呼ばれる「データ暗号化鍵」を暗号化して受信者へ送信し、受信者はＫＥＫを用いてＤＥＫを復号化し、ＤＥＫを用いて暗号文を解読している。
【０００４】また、送信者は受信者の公開鍵を入手し、この公開鍵をＫＥＫとして暗号化したＤＥＫを受信者へ送付し、送信者と受信者との間でＤＥＫを共有する方法もある。これら暗号化鍵の管理はカードによる方法もあるが、鍵情報の変質や紛失の危険もある。一般には、鍵サーバによって移動局毎に管理している。
【０００５】図１１に、鍵サーバーを使用する移動局と固定局の暗号通信の手順を示す。鍵サーバは鍵管理テーブルに移動局Ａの鍵Ｋ１、移動局Ｂの鍵Ｋ２と、全移動局の鍵を管理している。鍵Ｋ１を保持している移動局Ａが固定局と通信する場合、①移動局Ａの識別子による通信要求を発行し、②固定局は鍵サーバに移動局Ａの鍵を問合せ、③鍵サーバーは固定局に移動局Ａの鍵Ｋ１を応答し、④固定局は鍵Ｋ１（またはデータＫ１を種に生成した鍵Ｋ１１）を用いて移動局Ａに暗号通信を行ない、⑤移動局Ａは鍵Ｋ１（またはデータＫ１から解読した鍵Ｋ１１）を用いて暗号文を復号し、鍵Ｋ１（または鍵Ｋ１１）を用いた暗号文で固定局と通信する。
【０００６】なお、鍵情報は漏洩（盗聴・解読）による不正使用を防止するために、定期的または必要に応じてバージョンアップされる。鍵サーバが管理する鍵情報は移動局に固有の鍵または移動局に共通の鍵で、後者の場合は移動局毎に使用中の鍵バージョンが管理される。つまり、図９に例示した鍵Ｋ１，Ｋ２は固有情報でも、バージョン情報でもよい。
【０００７】
【発明が解決しようとする課題】上述のように、暗号通信の鍵情報を鍵サーバによって管理する方式では、固定局は移動局からの通信要求の度に使用する鍵をサーバに問合せするので、移動局と固定局間の通信開始までに時間がかかり、またサーバから固定局へＫＥＫやＤＥＫの鍵情報を直接に送信するので漏洩の危険も高い。
【０００８】特に、ＥＴＣでは料金収受に用いる無線電波の混信を防ぐために、通信領域を狭く設定する必要がある。一方、自動料金収受を行なう車両は停止することなく料金所を通過させる運用となるので、固定局と移動局との間の通信可能な時間はごく短い。例えば、車両が４ｍの通信領域を１８０ｋｍ／ｈの高速で走行した場合、通信可能な時間はわずか８０ｍｓである。従って、サーバによる鍵管理方式では、車両と料金所間の高速応答が困難なため、高速通過による料金収受が不可能になるので、料金所での渋滞解消に役立たなくなる。

【０００９】しかし、不特定多数の移動局の鍵情報をサーバに代わって固定局が管理することは、従来の技術では不可能である。なぜならば、個々の移動局が全国のどの料金所へ進入して通信を開始するか分からないので、各固定局は全移動局の鍵情報の管理が必要になるからである。移動局が共通鍵を使用する場合でも、移動局の鍵バージョンは個々の車検時などに更新されるので、複数の鍵バージョンを共用可能に運用する必要があり、固定局の管理は困難となる。

【００１０】また、使用中の鍵バージョンに不正使用が発覚した場合、被害のあった移動局への緊急対策はできても、その鍵バージョンを使用している他の多数の移動局に対しては緊急に対応できず、被害の拡大する恐れがある。

【００１１】本発明の目的は、従来の暗号文を含む移動通信の問題点を克服し、鍵情報の漏洩の危険が少なく高応答で通信を開始でき、あるいは緊急時の鍵更新が簡単に行なえる移動通信方法を提供することにある。

【００１２】また、鍵サーバの不要なシンプルで、高セキュリティの移動通信システムを提供することにある。さらに、短時間（高速通過中）に確実に料金収集（課金処理）のできる有料道路の自動料金収受システムを提供することにある。

【００１３】

【課題を解決するための手段】上記目的を達成するための本発明は、固定局と移動局の双方向の暗号通信の暗号化または復号化に用いる鍵（暗号鍵）を複数の移動局で共有可能とし、かつ前記暗号鍵の複数のバージョンを共用可能とする移動体通信方法において、移動局は固定局への通信要求時に、自局の使用可能な暗号鍵のバージョンを送信すると共に、このバージョンが固定局からの応答に含まれることを確認し、固定局は移動局からの受信バージョンが自局の管理する鍵情報に含まれるかチエックし、含まれる場合は当該バージョンを使用鍵に決定して前記通信要求を発信した移動局に応答すると共に、通信中、当該移動局の識別子とその使用鍵を対応付けて管理することを特徴とする。

【００１４】上記の固定局は、移動局からの受信バージョンが自局の管理する鍵情報に含まれていない場合は、鍵情報の一つまたはダミーのバージョンを移動局に応答し、当該移動局は、固定局からの応答バージョンが自局で使用可能な場合は、この応答のバージョンを使用鍵として、通信要求を再送信することを特徴とする。この結果、再送のバージョンが固定局で使用鍵に認められ、通信中管理される。

【００１５】この発明によれば、固定局は複数の移動局との間で、共通鍵の複数の鍵バージョンを混乱なく共用でき、固定局自身で使用鍵を決定できるので、即座に通信を開始できる。

【００１６】また、本発明は、各移動局及び固定局がそれぞれ自局の使用可能なバージョンの暗号鍵を、通常用と代替用の鍵用途に対応した一対の鍵（通常鍵と代替鍵）により管理し、移動局は固定局への通信要求時に、自局の使用可能な暗号鍵のバージョンを送信すると共に、固定局からの応答に含まれるバージョンと鍵用途をチエックし、応答のバージョンが自局と同一で鍵用途が通常用の場合は、自局の通信に使用する暗号鍵を前記通常鍵のままとし、固定局は移動局からの受信バージョンが自局の管理する複数のバージョンに含まれるかチエックし、含まれる場合は前記通常鍵の有効／無効をチエックし、有効の場合は当該通常鍵を使用鍵に決定して当該バージョンと鍵用途（通常用）を前記通信要求を発信した移動局に応答すると共に、通信中、当該移動局の識別子とその使用鍵を対応付けて管理することを特徴とする。

【００１７】また、上記の固定局は、移動局からの受信バージョンが自局の管理するバージョンに含まれかつ前記通常鍵が無効の場合に、当該通常鍵と対をなす代替鍵を使用鍵に決定して当該バージョンと鍵用途（代替用）を前記通信要求を発信した移動局に応答すると共に、通信中、当該移動局の識別子とその使用鍵を対応付けて管理し、当該移動局は、固定局から応答の鍵用途が代替用の場合に、自局の通常鍵を無効とし、それと対をなす代替鍵を自局の暗号通信の使用鍵とすることを特徴とする。

【００１８】さらに、上記の固定局における前記通常鍵の有効／無効の管理は、上位装置から指定されたバージョンの鍵用途変更指示を受信したときに、当該通常鍵を無効とすることを特徴とする。

【００１９】この発明によれば、不正使用が発覚した場合等に鍵バージョンの通常鍵を無効にし、各移動局が保持している代替鍵への切り替えを、暗号鍵を送信することなく通信中のオンライン処理できるので、緊急な対応が高セキュリティに実行できる。なお、通常鍵と代替鍵（実施例では緊急鍵）の対による方式を、以下では対称鍵暗号方式と呼ぶ。

【００２０】なお、上記で移動局から通信要求時に自局で使用する鍵のバージョンと鍵用途を送信し、固定局で使用を決定したバージョンのみを応答するようにしてもよい。これによれば、固定局の鍵決定処理がさらに簡単化される。

【００２１】上記移動体通信方法を適用する本発明の移動体通信システムは、固定局と移動体上に搭載される複数の移動局を備え、移動局は、自局の通信に使用する鍵バージョンと鍵を含む鍵情報を格納する鍵情報データベースと、固定局への通信要求時に自局の鍵バージョンを送信すると共に、固定局からの応答に含まれる鍵バージョンと対照して自局の使用鍵を管理する鍵管理処理手段を設け、固定局は、移動局との通信に使用する複数の鍵バージョンとその鍵を含む鍵情報を格納する鍵情報管理

データベースと、移動局から受信した鍵バージョンが前記データベースに含まれる場合にこの鍵バージョンの鍵を使用鍵に決定して、当該鍵バージョンを移動局に応答する鍵管理制御処理手段と、通信中の移動局の識別子とその使用鍵を対応付けて管理する通信鍵情報データベースを設けることを特徴とする。

【００２２】また、固定局及び移動局は、前記鍵情報として鍵バージョン毎に通常／代替の鍵用途と対応する一対の通常鍵と代替鍵を含み、かつ固定局には、上位からの鍵用途変更指示によって該当鍵バージョンの通常鍵の使用を無効にする管理機能を有し、固定局の前記鍵管理制御処理手段は、移動局から受信した鍵バージョンの通常鍵が無効の場合に対の代替鍵を使用鍵に決定してその鍵バージョンと鍵用途（代替）を移動局に応答し、移動局の前記鍵管理処理手段は固定局から応答の鍵用途が代替用の場合に鍵情報データベースの通常鍵を無効にすることを特徴とする。

【００２３】あるいは、固定局は前記鍵情報として鍵バージョン毎に通常の鍵用途となる通常鍵のみを含み、かつ上位から鍵用途変更指示による鍵バージョンと鍵用途が代替の代替鍵を受信して管理すると共に当該通常鍵の使用を無効にする管理機能を有してなることを特徴とする。

【００２４】上記の移動体通信システムの一適用例は有料道路の自動料金収受システム（ＥＴＣ）であり、固定局は料金所または路側に設けられる通信装置、移動局は有料道路を利用する車両に搭載される通信装置として構成される。

【００２５】本発明の移動体通信システムは鍵サーバを不要とするので、システム構成が簡素化するとともに、高セキュリティを確保できる。また、固定局と移動局間の通信が高速処理できるので、有料道路のＥＴＣの処理時間を短縮し、高速通過での料金収受が可能になる。

【００２６】

【発明の実施の形態】以下、本発明の一実施形態による移動通信方法とそのシステムについて、図面を参照しながら詳細に説明する。なお、各図を通して同等の構成要素には同一の符号を付している。

【００２７】図１０に、本発明を適用する有料道路の自動料金収受システムの概略の構成を示す。料金所に配置されたＥＴＣの固定局１００は、自動料金専用レーン２００の上部または側部に設置されたアンテナ１１０を介して、破線で示す通信エリア２１０内に進入した車両３００の搭載する移動局３１０との間で、秘密情報を暗号化して無線交信し、料金を自動徴収して上位装置へ報告する。

【００２８】アンテナ１１０のカバーする通信エリア２１０の延長は、他車との混信を防止するために高々数mである。このため、高速で通過する車両の移動局３１０と約０．１秒以下で交信を終了しなければならず、固定局１００と移動局３１０間の暗号通信には高速の応答が必要になる。

【００２９】図１は、本発明の一実施例による移動通信システムの構成図である。移動体に搭載された通信装置（移動局）１、移動局１と通信する路側に設置された通信装置（固定局）２、移動局１と固定局２を結ぶ通信路３から構成される。通信路３は無線、有線を問わないが、本実施例ではアンテナを介した無線による。以下では、移動局１と固定局２間の暗号通信を説明するが、秘密情報のみを暗号化して平文と組合せる場合も含む。また、暗号化／復号化のための鍵は上述の「データ暗号化鍵（ＤＥＫ）」を指すが、「鍵暗号化鍵（ＫＥＫ）」でもよい。

【００３０】移動局１は、平文の送信情報や受信情報及び鍵関連情報（鍵は含まない）を蓄えている通信用ＤＢ４、通信用ＤＢ４に蓄積されている固定局２からの鍵関連情報を読み出し、固定局２との通信に使用する鍵の決定と、鍵情報ＤＢ６の鍵情報（鍵を含む）の更新を行なう鍵管理処理部５、暗号化または復号化に用いる鍵（対称鍵）を含む鍵情報を格納する鍵情報ＤＢ６、通信用ＤＢ４の送信情報と鍵情報ＤＢ６の鍵を読み出し、送信情報を暗号文にする暗号化処理部７、この暗号文を通信路３へ送信しまた通信路３から暗号文を受信する通信処理部８、通信路３から受信した暗号文を鍵情報ＤＢ６の鍵を用いて復号し、復号化した平文の受信情報を通信用ＤＢ４へ格納する復号化処理部９、これら各部の起動を制御する制御処理部１０から構成されている。

【００３１】固定局２は、通信路３から暗号文を受信または送信する通信処理部８、送信路３から受信した暗号文を鍵情報ＤＢ１３から読み出した鍵を用いて復号化する復号処理部９、復号化された受信情報や平文の送信情報を蓄える通信用ＤＢ１１、固定局２の暗号通信でサポートする全ての鍵情報を格納する鍵情報管理ＤＢ１２、通信中の移動局毎の使用鍵を格納する鍵情報ＤＢ１３、通信用ＤＢ１１から移動局１の受信情報を読み出し、移動局１からの鍵関連情報と鍵情報管理ＤＢ１２に登録されている鍵情報を対照して移動局の鍵の有効／無効を判定し、判定結果に応じて移動局に応答する鍵関連情報を通信用ＤＢ１１へ格納する鍵管理制御処理部１４、鍵情報ＤＢ１３に格納された使用鍵を用い、移動局に送信する送信情報を暗号化する暗号化処理部７、これら各部の処理を起動する制御処理部１６から構成されている。

【００３２】以下では、対称鍵暗号方式による実施例によって、各部の動作を詳細に説明する。図２に、移動局の鍵情報データベースの構成を示す。対称鍵暗号方式の場合、鍵情報ＤＢ６に格納される鍵情報は、移動局が使用する鍵バージョン２１、対称鍵の通常または緊急の用途を示す鍵用途２２、暗号化または復号化に用いる鍵（対称鍵）２３、対称鍵２３の有効／無効を示す有効フラグ２４から構成される。図示例は、バージョン「Ｖ

1」に鍵用途が「通常」の鍵「K1」と、鍵用途が「緊急」の鍵「K1'」が登録されて、共に「有効」である。

【0033】図3に、固定局の鍵管理情報データベースの構成を示す。鍵情報管理DB12は、固定局2がサポートする一つ以上の鍵バージョンの履歴を示し、鍵バージョン21毎に通常及び緊急の鍵用途22と鍵（対称鍵）23、対称鍵の有効／無効を示す有効フラグ24から構成されている。図示例は、バージョンV1に対称鍵K1，K1'、バージョンV2に対称鍵K2，K2'が登録され、全て有効にサポートされている。

【0034】図4に、固定局の鍵情報データベースの構成を示す。鍵情報管理DB13は、通信中の移動局から受信した移動局識別子31と、この移動局との通信に用いる使用鍵32（鍵23）の対応を受信順に管理する。受信の終了した移動局の対応はDB13から消去され、管理順が更新される。これにより、同時に複数の移動局と異なるバージョンでの通信が可能になる。

【0035】図5に、移動局における対称鍵暗号方式の使用鍵決定処理のフローを示す。移動局1の鍵決定は固定局2との通信開始時に、制御処理部10の下で鍵管理処理部5が行ない、通常通信時と鍵緊急更新時の処理を含んでいる。

【0036】鍵管理処理5は、鍵情報DB6よりサポートしている鍵バージョンを読み込み（S101）、このバージョンを通信用DB4の鍵関連情報のエリアへ書き込む（S102）。鍵関連情報（ここでは、鍵バージョン）は通信要求のメッセージ（移動局の識別情報を含む）と共に、通信処理部8から固定局2へ送信される。その後、鍵管理処理5は固定局2からの鍵関連情報の受信を待つ（S103）。固定局2から受信した鍵関連情報（ここでは、鍵バージョンと鍵用途）を通信用DB4より読み出し（S104）、その鍵バージョンが自局でサポートされているか判定する（S105）。固定局2からの鍵バージョンが自局でサポートされていない場合は、制御処理部10へ異常通知を発行し（S106）、処理を終了する。

【0037】固定局2からの鍵バージョンが自局でサポートされている場合、つまり自局から送信した鍵バージョンと一致するとき、固定局2からの鍵用途22が緊急か否か判定する（S107）。緊急でなければ鍵用途は「通常」なので、自局の通常鍵を使用する通常通信であり、そのまま処理を終了する。一方、固定局からの鍵用途22が「緊急」の場合は自局の通常鍵が使用できないので、使用鍵を緊急鍵とするとともに鍵情報DB6における通常鍵の有効フラグ24を無効に更新する（S108）。この結果、当該移動局における以後の暗号化／復号化には、緊急鍵が使用される。

【0038】図6に、固定局における使用鍵決定処理のフローを示す。固定局2は移動局1からの通信要求に対し、制御処理部15に起動された鍵管理制御処理部14が、対称鍵暗号方式によって移動局毎の使用鍵を決定する。

【0039】鍵管理制御処理14は、移動局1から通信要求とともに受信した鍵関連情報のバージョンを通信用DB11より読み出し（S201）、鍵情報管理DB12を検索して受信した鍵バージョンのサポートを確認する。つまり、移動局1のバージョンの通常鍵が有効か判定し、もし通常鍵が無効であればさらに緊急鍵が有効か判定する（S202）。

【0040】受信したバージョンの通常鍵が有効の場合は、この通常鍵を使用鍵に決定し、当該移動局の識別子と対応付けて鍵情報DB13へ登録する（S203）。さらに、移動局1へ送信する鍵関連情報として、先に移動局1から受信した鍵バージョンに鍵用途（通常）を付加して、通信用DB11へ書き込み（S206）、処理を終了する。また、通常鍵が無効で緊急鍵が有効の場合は、受信した鍵バージョンの緊急鍵を使用鍵に決定し（S204）、鍵情報DB13へ登録する。

【0041】さらに、受信した鍵バージョンの通常鍵と緊急鍵が共に無効の場合は、固定局2でサポートしている鍵バージョンとその通常鍵を使用鍵に選定し（S205）、選定した使用鍵のバージョンと鍵用途を移動局に応答する。移動局が固定局からのバージョンをサポートしている場合は、このバージョンを通信要求とともに再送することで、上記の一連の処理が繰り返され、当該バージョンの通常鍵が使用鍵として決定され、通信が可能になる。

【0042】しかし、通常の移動局は唯一のバージョンをサポートする管理が行なわれ、新バージョンへの更新と共に旧バージョンを無効にしている。このような場合には、移動局1の鍵決定処理はサポート無しと判定し（S105）、通信を打ち切る。従って、固定局2の鍵決定処理では処理S205を行なわずに、移動局から受信した鍵バージョンの対称鍵が共に無効の場合は、単にダミーのバージョンを応答するようにしてもよい。

【0043】図7に、通常通信で使用鍵を決定する場合の移動局と固定局間の処理の流れを示す。移動局1の鍵管理処理部5は、①鍵情報DB6より自局がサポートする鍵バージョンがV1であることを読み込み、②固定局2へ通信要求のメッセージ（識別子を含む、例えばN××1）と共にバージョンV1を送信する。③固定局2の鍵管理制御処理部14は、移動局1から受信したバージョンV1を用いて鍵管理情報DB12を検索し、バージョンV1をサポートしているか確認する。④バージョンV1のサポートを確認すると、バージョンV1の通常鍵K1を使用鍵に決定し当該移動局の識別子（N××1）と対応付けて鍵情報DB13へ登録する。また、⑤当該移動局へバージョンV1と鍵用途（通常）からなる鍵関連情報を送信する。なお、移動局1と固定局2の鍵決定

のための通信②，⑤で、鍵関連情報を暗号化してもよい。

【００４４】移動局１の鍵管理処理部５は、固定局２からの鍵関連情報によって自局のバージョンＶ１とその通常鍵Ｋ１の使用を確認する。次に、⑥移動局１は通信用ＤＢ４から平文の送信情報を暗号処理部７に読み込み、鍵情報ＤＢ６から読み出した使用鍵Ｋ１を用いて暗号化する。例えば、有料道路のＥＴＣシステムでは、料金引き落しのためのＩＣカード番号や残金額などが暗号化されて送信される。そして、⑧通信処理部８から固定局２に暗号文を送信する。⑨固定局２の復号処理部９は、受信した暗号文を鍵情報ＤＢ１３の識別子（Ｎ××１）に対応する鍵Ｋ１によって、平文に復号する。

【００４５】これによれば、移動局の通信要求により固定局との間で使用鍵を決定する処理のみで、両者間の通信が即座に開始できるので、通信時間が約０．１秒以下に制限される有料道路のＥＴＣシステムにも適用可能である。また、暗号化／復号化に用いる使用鍵そのものは鍵関連情報に含まず、通信されないので、システムの高セキュリテイを確保できる。

【００４６】図８に、鍵緊急更新で使用鍵を決定する場合の移動局と固定局間の処理の流れを示す。移動局１の鍵管理処理部５は、①鍵情報ＤＢ６に有効管理されているバージョンＶ１を読み出し、②固定局２に送信要求メッセージと共に送信し、③固定局２の鍵管理制御処理部１４がバージョンＶ１のサポートを確認するまでは、通常通信の場合と同様である。④確認の結果、バージョンＶ１の通常鍵Ｋ１が無効、緊急鍵Ｋ１’が有効の場合、バージョンＶ１の緊急鍵Ｋ１’を使用鍵に決定し当該移動局の識別子（Ｎ××１）と対応付けて鍵情報ＤＢ１３へ登録し、⑤当該移動局へバージョンＶ１と鍵用途（緊急）からなる鍵関連情報を送信する。

【００４７】移動局１の鍵管理処理部５は、⑥固定局２からの鍵用途によって自局の通常鍵Ｋ１の無効を知ると、鍵情報ＤＢ６の通常鍵Ｋ１の有効フラグを無効にする。暗号処理部７は平文の暗号化に際し、鍵情報ＤＢ６で有効に管理されているＫ１’を使用する。移動局１から固定局２への暗号文の送信（⑧）以降は、通常通信の場合と同様である。なお、移動局１から固定局２へ通信要求時の鍵関連情報に鍵バージョンと共に鍵用途を含めると、緊急鍵を使用している固定局側の鍵決定処理を簡単化できる。このとき、固定局２から移動局１へ応答する鍵関連情報は鍵バージョンのみでよい。

【００４８】ところで、固定局における通常鍵の有効／無効の管理は、上位装置から特定の鍵バージョンに対する無効指示によって行なわれる。すなわち、移動局の利用料金などを清算する中央装置などで、一つの移動局に対して複数の固定局から物理的に不可能な同時的利用の事実を検出した場合や、ユーザからの苦情申立てが有った場合に、不正使用が発生したと判断して通常鍵の無効を指示する。

【００４９】図９に、固定局における通常鍵の無効化の処理フローを示す。鍵管理制御処理部１４は、上述した通信鍵決定の処理機能（図６）の外に、通常鍵無効化の処理機能を有している。まず、上位装置からの鍵用途変更指示の受信を待つ（Ｓ３０１）。上位装置から、鍵バージョンを指定した鍵用途の変更指示を受信すると、指定されたバージョンの通常鍵を無効にし、鍵情報管理ＤＢ１２の当該有効フラグを無効に設定する（Ｓ３０２）。なお、本処理は、鍵決定処理に対する割込みによって処理してもよい。

【００５０】本実施例によれば、不正使用が発覚した鍵バージョンの通常鍵を無効にし、各移動局が保持している緊急鍵への切り替えをオンラインで処理できるので、不正使用による被害の拡大を防止しながらシステムの通常の運用を維持できる。また、緊急鍵のデータを互いに通信することなく切り替えるので、高セキュリティな対応が可能になる。

【００５１】例えば、有料道路のＥＴＣシステムでは、通常の移動局のバージョン更新は定検時などとなるので、不正による被害の拡大によりシステム停止に追い込まれる恐れがある。しかし、本実施例によれば、緊急鍵への切り替えが通常利用の通信中にオンラインで自動処理されるので、システムにもユーザにも負担がなく使い勝手がよい。

【００５２】以上の実施例では移動局と固定局の暗号通信の暗号鍵に対称鍵を用いたが、本発明の移動通信は暗号鍵に非対称鍵、または暗号アルゴリズムを変更するアルゴリズム鍵等によっても実現できる。

【００５３】また、上述した対称鍵暗号方式では、移動局と固定局に予め通常鍵と緊急鍵からなる対称鍵を用意している。しかし、固定局は通常鍵のみをインストールしておき、上位装置から固定局への鍵用途変更指示に付加して当該バージョンの緊急鍵を送信するようにしてもよい。これにより、固定局での盗難等による緊急鍵の露見を防止できる。なお、上位装置からの鍵情報の通信による漏洩の危険が伴うので一時的な緊急対策とし、抜本的には移動局のバージョン更新が必要になる。

【００５４】

【発明の効果】本発明の移動体通信方法によれば、固定局と複数の移動局とで共通鍵の複数のバージョンを共用する場合に、移動局の通信要求時のバージョンを確認して固定局自身で使用鍵を決定できるので、移動局との通信を速やかに開始できる。

【００５５】また、対称鍵暗号方式を採用するので、不正使用が発覚した場合等に各移動局が保持している代替鍵への切り替えを、暗号鍵を送信することなくオンライン処理で実効できるので、不正使用の被害の拡大を防止できる。

【００５６】本発明の移動体通信システムによれば鍵サ

ーバを不要とするので、システム構成が簡素化するとともに、高セキュリティを確保できる。また、緊急時の鍵切り換えを通信中に自動処理するので使い勝手がよい。

【図面の簡単な説明】

【図１】本発明の一実施例による移動体通信システムの構成図。

【図２】対称鍵暗号方式を用いた移動局の鍵情報ＤＢのデータ構成図。

【図３】対称鍵暗号方式を用いた固定局の鍵管理情報ＤＢのデータ構成図。

【図４】固定局の通話中の使用鍵を管理する鍵情報ＤＢの構成図。

【図５】移動局の対称鍵暗号方式による使用鍵の決定処理を示すフロー図。

【図６】固定局の対称鍵暗号方式による使用鍵の決定処理を示すフロー図。

【図７】移動局と固定局間の通常の鍵決定の処理とデータの流れを示す説明図。

【図８】移動局と固定局間の鍵緊急更新の処理とデータの流れを示す説明図。

【図９】上位指示により、固定局の通常鍵無効化処理を示すフロー図。

【図１０】有料道路の自動料金収受システム（ＥＴＣ）の概略の構成図。

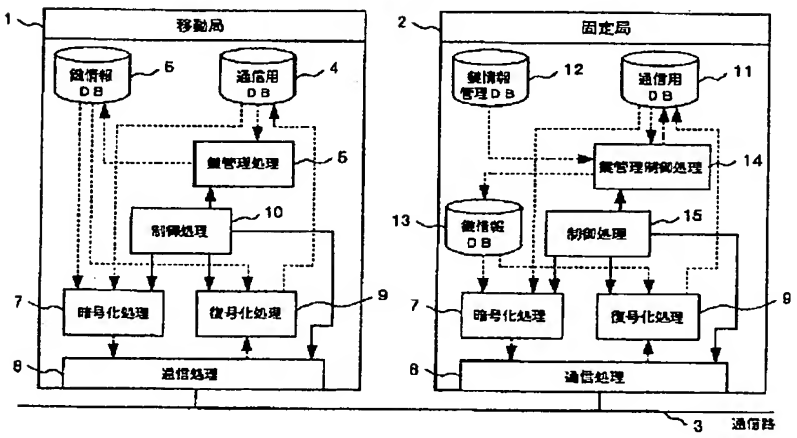
【図１１】鍵サーバ問合せによる鍵決定動作を示す従来の移動体通信システムの説明図。

【符号の説明】

１…移動局、２…固定局、３…通信路、４…通信用ＤＢ、５…鍵管理処理部、６…鍵情報ＤＢ（移動局側）、７…暗号化処理部、８…通信処理部、９…復号化処理部、１０…制御処理部（移動局側）、１１…通信用ＤＢ、１２…鍵情報管理ＤＢ、１３…鍵情報ＤＢ（固定局側）、１４…鍵管理制御処理部、１６…制御処理部（固定局側）、２１…鍵バージョン、２２…鍵用途、２３…対称鍵、２４…有効フラグ、３１…移動局識別子、３２…使用鍵、１００…固定局、１１０…アンテナ、２００…専用レーン、２１０…通信エリア、３００…車両、３１０…移動局。

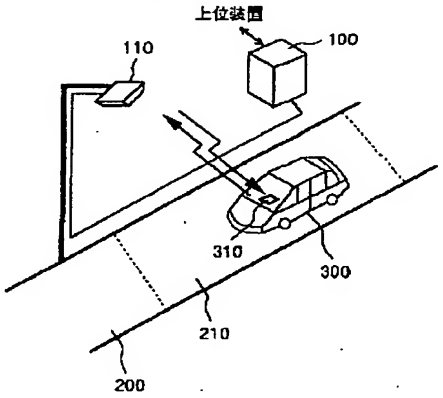
【図１】

図 1



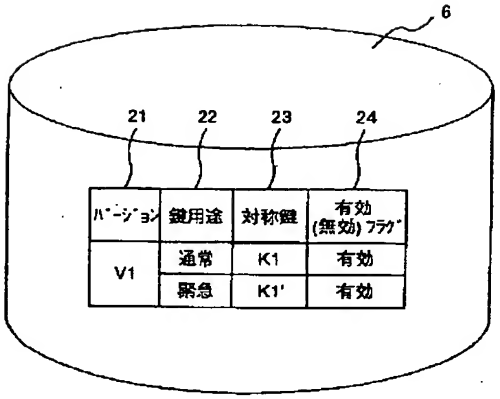
【図１０】

図 10



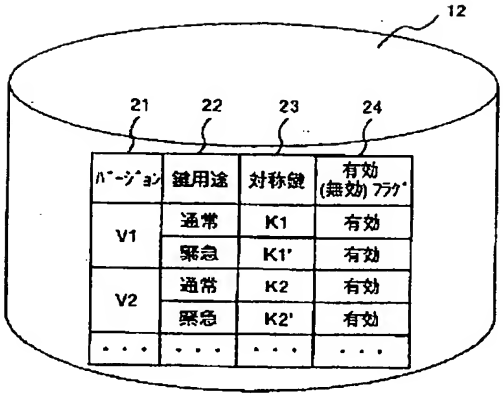
【図２】

図　2



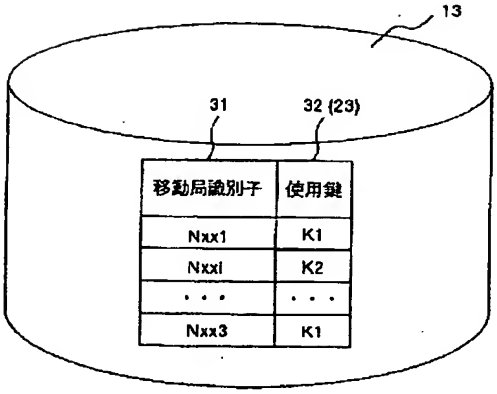
【図３】

図　3



【図４】

図　4



【図５】

図　5